Mapbox Data Processing Addendum

(Last Revised August, 2023)

How This DPA Is Executed

This Data Processing Addendum ("**DPA**") is hereby incorporated by reference into the written or electronic Master Services Agreement or Terms of Service ("**Agreement**") to reflect the Parties' agreement regarding the Processing of Personal Data and is made and entered into effective as of the later of the Agreement dates executed by authorized representatives of the Parties ("**Effective Date**") and between:

The company set forth in the Agreement ("**Customer**"); and

Mapbox, Inc. ("**Mapbox**"), a company constituted under the laws of Delaware with an address of 740 15th Street NW, 6th Floor, Washington DC 20005 (together, the "**Parties**" and the "**Party**" shall be construed accordingly).

About This DPA

1. This DPA consists of two parts: the main body of this DPA and Schedules A, B, C and D.
2. For avoidance of doubt, with respect to transfers of Personal Data that is subject to the laws of Europe, the Parties are deemed to have signed the Standard Contractual Clauses, which are incorporated herein by reference and are deemed completed as set forth in Schedule A.
3. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

Data Processing Terms

1. Definitions

1.1. **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

1.2. **"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such processing are determined by union or member state law, the Controller or the specific criteria for its nomination may be provided for by union or member state law.

1.3. **"Data Subject"** means an identified or identifiable living natural person to whom the Personal Data relates. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.4. **"Data Protection Laws"** means laws and regulations, including laws and regulations of Europe and its countries and member states and the United States and its states, applicable to Processing of Personal Data.

1.5. **"Europe"** means the European Union, the European Economic Area, Switzerland and the United Kingdom.

1.6. **"Personal Data"** means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, or relating to an identified or identifiable natural person, or within the scope of personal information or personal data under applicable Data Protection Laws.

1.7. **"Personal Data Breach"** means a breach of this DPA leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, Personal Data transmitted, stored or otherwise Processed by or for Mapbox on behalf of Customer.

1.8. **"Processor"** means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

1.9. **"Processing"** or **"Processes"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.10. **"Purpose"** means to provide, test, maintain/support, secure and improve the Mapbox products/services, to prevent fraud, misuse and cyberattacks, to anonymize & calculate de-identified aggregate statistics, and for account administration/ billing purposes.

1.11. **"Sell"** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject's Personal Data by a business to a third party for monetary or other valuable consideration, as outlined in the CCPA.

1.12. **"Standard Contractual Clauses"** or **"Clauses"** means the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

1.13. **"Sub-processor"** means any Processor engaged by Mapbox or its Affiliates.

2. Customer's Instructions & Processing Operations

2.1. **Roles of the Parties and Details of Processing.** The Parties agree that as it relates to Personal Data in Schedule B, the Customer is the Controller, Mapbox is the Processor, and Mapbox Affiliates are Sub-processors in addition to any other Sub-processors noted in accordance with Section 4 of this DPA. Customer instructs Mapbox to Process Personal Data on its behalf for the Purpose in accordance with this DPA.

2.2. **Customer's Processing of Personal Data.** Customer represents, warrants and covenants that with respect to Personal Data provided to Mapbox pursuant to this DPA, Customer: (a) complies with Data Protection Laws; (b) has lawfully obtained and recorded all necessary consents or other lawful basis required for Processing under this DPA; (c) has established a procedure for the exercise of the rights of the Data Subjects whose Personal Data is Processed; (d) ensures that it has assessed the technical and organizational measures implemented by Mapbox, as outlined in Schedule D; and (e) takes reasonable steps to ensure its compliance with the provisions of this DPA by its personnel and by any person Processing Personal Data on its behalf.

2.3. **Mapbox's Processing of Personal Data.** Mapbox shall Process Personal Data provided to Mapbox pursuant to this DPA on behalf of Customer and only in accordance with the Purpose, Customer's documented instructions herein, to comply with Customer's other reasonable instructions (email is acceptable) where such instructions are consistent with the Purpose, and as permitted by law and legal process or Data Protection Laws. Mapbox is prohibited from Selling such Personal Data or retaining, using or disclosing such Personal Data outside of the direct business relationship between the parties. If, in Mapbox's opinion, an instruction from Customer infringes Data Protection Laws or Mapbox can no longer comply with its obligations in this DPA, Mapbox shall promptly inform Customer. Mapbox certifies that it understands its obligations under the CCPA and complies with them.

2.4. **Data Protection Impact Assessment and Prior Consultation.** Upon Customer's request, Mapbox shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligations under Data Protection Laws to carry out a data protection impact assessment or prior consultation with a supervisory authority solely related to Customer's use of the Mapbox products/services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Mapbox.

2.5. **Confidentiality.** Mapbox shall maintain operational practices designed to ensure its personnel engaged in Processing Personal Data receive appropriate training and are bound by contractual or statutory confidentiality.

3. Data Subject Rights

3.1. Mapbox shall take appropriate technical and organization measures, in light of the Personal Data being Processed and insofar as it is possible, designed to support Customer's compliance with its obligation to fulfill its Data Subject rights requests in accordance with Data Protection Laws. To the extent legally permitted and where Customer can be identified in the request, Mapbox shall promptly notify Customer of Customer's Data Subjects' requests received by Mapbox such as the right to access, right to rectification, right to deletion, right to data portability, and right to object to Processing and Mapbox shall not respond to the Data Subject directly beyond redirecting them to Customer.

4. Sub-processors

4.1. **Appointment of Sub-processors.** Customer acknowledges and agrees that Mapbox Affiliates may be engaged as Sub-processors of Mapbox and that Mapbox and its Affiliates may engage third-party Sub-processors to provide the Mapbox products/services. To the extent Personal Data is Processed, Mapbox or its Affiliate shall enter into a written agreement with the Sub-processor that contains provisions no less protective than those in this DPA. Mapbox shall be liable for all acts and omissions of its Sub-Processors Processing under this DPA to the same extent Mapbox would be liable if performing Processing of each Sub-Processor directly under the terms of this DPA.

4.2. **List of current Sub-processors and notification of new Sub-processors.** Customer hereby consents to Mapbox's use of Sub-processors and their respective locations of Processing, including such locations' Data Protection Laws relating to government access to Personal Data, published here: https://www.mapbox.com/legal/subprocessors as amended from time to time. Customer shall be notified of new Sub-processors by subscribing at the bottom of this page: https://www.mapbox.com/legal/subprocessors, providing Customer's preferred company email, and clicking "get updates." In the event that Mapbox is required to implement an emergency change of Sub-processor, Mapbox agrees to inform Customer as soon as is reasonably practicable before or after such a change occurs.

4.3. **Objection right for new Sub-processors.** Customer may object to Mapbox's use of a new Sub-processor provided such objection is based on Data Protection Laws and provided that such objection is in writing and sent to privacy@mapbox.com within fifteen (15) days of Mapbox's notice of new Sub-processor. If Mapbox, in its sole discretion, is unable to make an accommodating change within a reasonable period of time, which shall not exceed ninety (90) days (the "Cure Period"), as customer's sole remedy, either party may terminate the part of the Mapbox products/services that cannot be provided by Mapbox without the use of the objected-to new Sub-processor by providing written notice to the other party within five (5) business days after the end of the Cure Period.

5. Security

5.1. **Controls to Protect Personal Data.** In determining the technical and organizational measures required by this DPA, Mapbox takes into account the state of the art, the costs of implementation and the nature, scope, context and Purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Mapbox implements, as applicable, the technical and organizational measures outlined in Schedule D and the specific security measures detailed at: https://www.mapbox.com/platform/security/ as amended from time to time.

5.2. **Personal Data Breach.** Mapbox shall promptly notify Customer of any Personal Data Breach. Mapbox shall make reasonable efforts to identify the cause of such Personal Data Breach and take steps that Mapbox deems necessary and reasonable to remediate. Such notification shall contain: (a) a description of the nature of the breach (including, where possible, categories and approximate number of Data Subjects and Personal Data records concerned); (b) its likely consequences; (c) the measures taken or proposed to address the breach; and d) contact information for a point person from whom more information can be obtained. To the extent it is not possible for Mapbox to provide all information at the same time, it may do so in phases without undue further delay.

5.3. **Audit.** Mapbox agrees, at the request of Customer, to submit to an audit to ascertain Mapbox's compliance with this DPA and Data Protection Laws provided such audit shall be: (a) carried out no more than once in any 12 month period (unless otherwise required by applicable Data Protection Laws); (b) for cause with reasonable notice and during regular business hours and in a manner which does not disrupt Mapbox's business; (c) under a duty of confidentiality, where permitted by Data Protection Laws; and (d) conducted by one of the 'big 4' auditing firms appointed by Customer and accepted by Mapbox. The scope of such an audit shall be agreed in advance and, where required by Data Protection Laws, may include an inspection where Mapbox makes available to Customer all information necessary to demonstrate compliance with the obligations laid down in Data Protection Laws. Customer shall bear its own costs, the fees of any auditor and any documented expenses incurred by Mapbox in complying with this Section 5.3. If unauthorized use of Personal Data is found, Customer can take reasonable and appropriate steps to stop and remediate such unauthorized use, as required by Data Protection Laws. This paragraph only applies to the extent expressly required under Data Protection Laws.

6. Government Access Requests

6.1. Mapbox shall notify Customer of any legally binding request for disclosure of Customer's Personal Data by a law enforcement or supervisory authority, to the extent permitted by law and legal process.

7. Deletion of Personal Data

7.1. Mapbox shall only retain Personal Data for so long as it has a business need to fulfill the Purpose. Upon Customer's written request within thirty (30) days after Agreement termination or expiration, Mapbox shall delete all Personal Data unless prevented by or needed to comply with applicable law, or needed for a lawful basis, from destroying all or part of such Personal Data. In such a case, Mapbox agrees to uphold its obligations in this DPA and preserve the confidentiality of Personal Data retained by it and that it shall only Process such Personal Data after such date for compliance with the laws it is subject to or its use for an established lawful basis.

8. European Data Transfers

8.1. For transfers of Personal Data from Europe to countries where the European Commission has not determined, on the basis of Article 45 of Regulation (EU) 2016/679, whether such country offers an adequate level of data protection, the Standard Contractual Clauses are incorporated herein and completed as set forth in and subject to Schedule A.

9. Miscellaneous The governing law, venue, and dispute resolution provisions of the Agreement shall apply to this DPA.In the event of any conflict or inconsistency between this DPA and the Agreement pertaining to the Processing of Personal Data on behalf of Customer, this DPA shall prevail. Without limiting liability that either Party may owe directly to the Data Subject, each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA is subject to the 'Limitation of Liability' section in the Agreement. This DPA shall only become legally binding between Customer and Mapbox as of the Effective Date.

Schedule A

Additional Terms to Standard Contractual Clauses

With respect to transfers of Personal Data that are subject to the laws of Europe, the Parties are deemed to have signed the Standard Contractual Clauses, which are incorporated herein by reference and are deemed completed as follows:

1. **Instructions.** This DPA and the Agreement are Customer's complete and final instructions as of the Effective Date to Process Personal Data. Any additional or alternate instructions must be agreed upon separately in writing (email is sufficient). For the purposes of Clause 8.1 of the Standard Contractual Clauses, the Processing described in Section 2 of this DPA is deemed an instruction by the Customer to Mapbox to Process Personal Data.
2. **Conflict.** In the event of any conflict or inconsistency between the body of this DPA, this Schedule, and any of its Schedules, and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.
3. **Docking Clause.** The optional language under Clause 7 shall not apply.
4. **Security of Processing.** Pursuant to Clause 8.5(d), Personal Data Breaches shall be carried out in accordance with Section 5.2 of this DPA.
5. **Audits and Certifications.** The Parties agree that the audits described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Section 5.3 of this DPA.
6. **Sub-processors.** Pursuant to Clause 9(a), Option 2 of the Standard Contractual Clauses, Mapbox has Customer's general authorisation to engage Sub-processor(s) from the agreed list in Section 4 of this DPA. Appointment and notification of new Sub-processors shall be carried out in accordance with Section 4 of this DPA.
7. **Copies of Sub-processor Agreements.** The Parties agree that the copies of the Sub-processor agreements that may be provided by Mapbox to Customer pursuant to Clause 9(c), of the Standard Contractual Clauses shall have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Mapbox beforehand; and, that such copies shall be provided by Mapbox in a manner to be determined in its discretion and only upon written request by Customer.
8. **Data Subject Right.** Pursuant to Clause 10, Module 2, 3 and 4 of the Standard Contractual Clauses Data Subject rights shall be carried out in accordance with Section 3 of this DPA.
9. **Redress.** Pursuant to Clause 11 of the Standard Contractual Clauses, and subject to Section 3 of this DPA, Mapbox shall inform Data Subjects on its website (privacy policy or like policy or document) of a contact point authorised to handle complaints and all Data Subject requests shall be carried out in accordance with Section 3 of this DPA.
10. **Liability.** Pursuant to Clause 12, of the Standard Contractual Clauses, liability shall be carried out in accordance with Section 9 of this DPA.
11. **Court-review safeguard:** Pursuant to Clause 15, should Mapbox receive demands for data access through national security process for data related to Customer or its end users of which Mapbox is a Processor, to the extent Mapbox concludes there are reasonable grounds to consider that the request is unlawful under the laws of the third country of destination, it shall use commercially reasonable legal mechanisms to challenge such demands as well as any non-disclosure provisions attached thereto.
12. **Notice of demand:** To the extent legally permissible, Mapbox shall promptly notify the Customer if it receives demands for data access through national security process for data related to Customer or its end users of which Mapbox is a data Processor and shall make all commercially reasonable legal efforts to refrain from providing data until such reasonable time when the Customer has, or reasonably should have, had an opportunity to challenge such demands.
13. **Certification of Deletion.** The Parties agree that the certification of deletion of Personal Data that is

described in Clause 16(d) of the Standard Contractual Clauses shall be provided by Mapbox to Customer in email form upon Customer's written request.

14. **Appendix:**
    a. The contents of Section 1 of Schedule B shall form Annex I.A to the Standard Contractual Clauses
    b. The contents of Sections 2 to 8 of Schedule B shall form Annex I.B to the Standard Contractual Clauses
    c. The contents of Section 9 of Schedule B shall form Annex I.C to the Standard Contractual Clauses
    d. The contents of Section 5.1 of this DPA and Schedule B, Section 10 shall form Annex II to the Standard Contractual Clauses
15. **Data Exports from the United Kingdom and Switzerland under the Standard Contractual Clauses.** In the case of any transfers of Personal Data from the United Kingdom that is exclusively subject to United Kingdom Data Protection Laws ("UK Data Protection Laws"), and/or in case of any transfers of Personal Data from Switzerland that is exclusively subject to Swiss Data Protection Laws ("Swiss Data Protection Laws"), then general and specific references or obligation in the Standard Contractual Clauses to GDPR or EU or Member State Law shall refer to the equivalent reference in either UK Data Protection Laws or Swiss Data Protection Laws, as applicable. In respect of data transfers governed by UK Data Protection Laws, the Parties are hereby deemed to have entered the United Kingdom Information Commissioner's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0 of which is available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, which are completed as set forth in Schedule C. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

16. Governing Law. Pursuant to Clause 17 of the Standard Contractual Clauses, the SCCs shall be governed by the law of the courts of Ireland.

17. Choice of Forum and jurisdiction. Pursuant to Clause 18 of the Standard Contractual Clauses, any dispute arising from the SCCs shall be resolved by the courts of Ireland.

Schedule B

Details of the Processing Activities and Transfer (where applicable)

1. List of the Parties

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: **Customer**
Address: **As identified in the Agreement**
Contact person's name, position and contact details: **As identified in the Agreement**
Activities relevant to the data transferred under these Clauses: **See Schedule B, Section 6**
Signature and date: **Effective Date**
Role (controller/processor): **Controller or Processor**

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: **Mapbox, Inc.**
Address: **740 15th Street NW, 6th Floor, Washington DC 20005**
Contact person's name, position and contact details: **privacy@mapbox.com**
Activities relevant to the data transferred under these Clauses: **See Schedule B, Section 6**
Signature and date: **Effective Date**
Role (controller/processor): **Processor**

2. Categories of Data Subjects

Depending on Customer's use of the Mapbox products/services, in its sole discretion, Customer may submit Personal Data relating to the following categories of Data Subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Customer, end users, employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)

3. Categories of Personal Data

Data Category	**Examples**
Identifiers	Such as randomly generated billing ID, session ID & feedback ID (if given), and IP address (to provide the service, for billing/security purposes and deleted after 30 days).
Commercial Information	Such as user agent, which may include an application ID (determined by the Mapbox customer to identify its application), Mapbox customer's account ID (so that Mapbox knows which company to bill) and Mapbox product name(s) and version(s). Such as data that an individual may upload to Mapbox products/services or otherwise provide to Mapbox in connection with support, or feedback that end users voluntarily contribute to Mapbox along with their associated contact information.
Internet or other electronic network activity	Such as timestamp accompanying received data elements, and an end user's abandonment of a given navigation route / use of an alternate navigation route. Such as connectivity and device data including device model and browser information, operating system, and contents of an API or SDK request.
Geolocation Data	Such as latitude and longitude, altitude, horizontal and vertical accuracy

	(an IP address is not associated with such geolocation data and the session ID association is broken within 24 hours.)

4. Special categories of data

Customer is not permitted to submit special categories of Personal Data to Mapbox through the Mapbox products/services, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data, health and/or sex life.

5. Frequency of the transfers

Continuous, depending on Customer's use of the Mapbox products/services.

6. Nature & Purpose of the Processing

The nature and purpose of Processing is to provide, test, maintain/support, secure and improve the Mapbox products/services, to prevent fraud, misuse and cyberattacks, to anonymize & calculate de-identified aggregate statistics, and for account administration/ billing purposes

7. Duration of Processing

Subject to Section 7 of this DPA, Mapbox shall Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing**.**

8. Sub-processor Transfers

In accordance with Schedule B, Section 6 above, the Sub-processor shall Process Personal Data as instructed by Mapbox. Subject to Section 4 of this DPA, the Sub-processor shall Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

9. Competent Supervisory Authority

Identify the competent supervisory authority/ies in accordance with Clause 13 of the Standard Contractual Clauses:

- Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.
- Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as the competent supervisory authority.
- Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: Irish Data Protection Commissioner shall act as the competent supervisory authority.
- Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws, the Information Commissioner's Office shall act as the competent supervisory authority.
- Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws

10. Technical and Organizational Measures

Mapbox shall maintain administrative, physical, and technical safeguards designed for protection of the security, confidentiality and integrity of Personal Data Processed by the Mapbox products/services, as described in Section 5.1 of this DPA and Schedule D.

Schedule C

The UK Standard Contractual Clauses shall be deemed completed as follows:

1. Table 1: The Parties details and key contacts are set forth in Schedule B1.
2. Table 2: The Approved Standard Contractual Clauses referenced in Table 2 shall be the Standard Contractual Clauses as set forth in Section 8 and Schedule A of this DPA.
3. Table 3: Annexes 1A, 1B, II and III are as set forth in as set forth in Schedules A & B of this DPA.
4. Table 4: Mapbox may end the UK Standard Contractual Clauses as set out in Section 19 of the UK Standard Contractual Clauses.
5. By entering into this DPA, the Parties are deemed to be signing the UK Standard Contractual Clauses.

Schedule D

Mapbox product/services Technical and Organizational Measures

No.	Measures	Description
1.	Measures of de-identification of personal data	Randomly generated non-persistent identifiers with regular rotation, where practical.
2.	Measures of encryption of personal data	Encryption in transit and at rest via TL 1.2 or industry standard equivalent.
3.	Measures for ongoing confidentiality, integrity, availability and resilience of processing systems and services	Operationalized technical and organisational measures designed to ensure the confidentiality, integrity, availability and resilience of processing systems and services such as strict access control with logging, limited data retention periods and regular third party pen testing.
4.	Measures for the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	We have SLAs for uptime of the Services. AWS shared responsibility model, see here, as may be updated from time to time: https://aws.amazon.com/compliance/shared-responsibility-model/
5.	Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures designed to ensure the security of the processing	Periodic internal verification, table top exercises and assessments.
6.	Measures for user identification and authorisation	With regard to system security, Mapbox uses multi-factor authentication and administrative controls, passwords for security.
7.	Measures for the protection of data during transmission	Encryption in transit and at rest via TL 1.2 or industry standard equivalent.
8.	Measures for the protection of data during storage	Encryption in transit and at rest via TL 1.2 or industry standard equivalent.
9.	Measures for physical security of locations at which personal data are processed	AWS shared responsibility model, see here, as may be updated from time to time: https://aws.amazon.com/compliance/shared-responsibility-model/
10.	Measures for events logging	In accordance with Mapbox Logging and Monitoring Policy.
11.	Measures for system configuration, including default configuration	AWS shared responsibility model, see here, as may be updated from time to time: https://aws.amazon.com/compliance/shared-responsibility-model/
12.	Measures for internal IT and IT security governance and management	Mapbox Head of Security managing • Identification of Strategic Objectives and Avoidance of Silos • Identification of Relevant Risks • Analysis and Prioritization of Mitigation Efforts • Mitigation • Tracking and Reviewing
13.	Measures for certification/assurance of processes and products	Mapbox software development policy, processes and procedures including configuration and testing guidelines required prior to release.
14.	Measures for data minimisation	Internal privacy reviews with analysis of each data element and its proposed use case.
15.	Measures for data quality	In accordance with Mapbox Backup and Restoration Policy - Production Environment.
16.	Measures for limited data retention	Internal privacy reviews with analysis of each data element and its proposed use case, including proposed retention period.
17.	Measures for accountability	Mapbox runs a global data protection program, based on privacy by design, which includes monitoring for upcoming privacy laws and regulations to assess whether its practices may need to be adjusted to

		maintain compliance; product/service privacy reviews; data breach response processes; and operationalized technical and organisational measures including strict access controls with logging, limited data retention, security audits and SOC2 certification, pseudonymization of personal data (where applicable), and encrypted IP addresses in transit and at rest.
18.	Measures for data portability and erasure	Mapbox has operationalized data subject rights request responses processes, including those to respond to a request for data portability of personal data.